21 July 2015 Study · Web & Cloud · Mobile Security

Apache Cordova Cryptography Plugin

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/apache-cordova-cryptography-plugin/

This project implements a cryptography plugin for the Cross-Platform Framework Apache Cordova. The plugin is currently available for Android only. The plugin implements the Web Crypto API . Therefore, cryptographic methods can be invoked using the interface provided by the Web Crypto API. The cryptographic methods are implemented natively and cryptographic keys are stored using the on-device key storage facilities. As many Android devices use a KeyStore backed by a Secure Element, this cryptography plugin provides protection against software attacks on the key material.

Implementation

During implementation we have focused on cryptographic methods, that require the storage of key material. Therefore, we do not provide implementations of hashing algorithms, as hash algorithms provided by the user agent can be used safely.

We have introduced so-called crypto providers. Thus multiple implementations of the Web Crypto API can be instantiated and used within a web application.

- Getting the crypto provider implemented within the Apache Cordova Plugin:

var cordovaCryptoApi = window.getCryptoProviderByName(“cordova-iaik”);

- Getting the crypto provider implemented within the user agent:

var w3cCryptoApi = window.getCryptoProviderByName(“w3c”);.

The Web Crypto API uses CryptoKey objects as key handles to the raw key material. We provide an extension of the CryptoKey object by adding the attribute „id“. The „id“ is used for mapping the key handle in JavaScript with the entry in the Android KeyStore. Therefore, when creating a new CryptoKey by calling

generateKey(...) or importKey(...) the additional attribute „id“ has to be added to the algorithm dictionary. The README.txt included within the cordova-crypto-plugin.zip file provides additional documentation on how to use the plugin.

The following table provides an overview of implemented cryptographic methods:

License

This project is licensed under EUPL Version 1.1. The Cordova Cryptography Plugin uses the IAIK-Toolkits IAIK-Java Cryptography Extension and IAIK ECC. For research and educational purpose SIC provides free licenses. See SIC Licenses for further information. The folder cordova-crypto-plugin/src/android/libs includes an evaluation version of the libraries.

This project uses the BouncyCastle implementation for the SCrypt Key Derivation function. BouncyCastle is licensed under the MIT license. BouncyCastle is included in the folder cordova-crypto-plugin/src/android/libs.